Transforming Cybersecurity

Transforming Cybersecurity, published by ISACA®, should be read in the context of *COBIT® 5 for Information Security* and the COBIT® 5 framework. *Transforming Cybersecurity* is a useful handbook for any cyber security practitioner, information security manager (ISM) or IT auditor. The book explains that cyber security is a management task and encompasses all that protects enterprises and individuals from attacks and breaches in a connected environment. The governance, management, and assurance of cyber security are iterative and evolving processes.

The focus of cyber security should be on advanced persistent threats (APTs), cyberwarfare and the impact on individuals. The tasks and responsibilities linked to cyber security are essential for an organization's survival and profitability. The integration of these tasks with COBIT would enable enterprises and individuals to harmonize security strategies in a systematic way.

Transforming Cybersecurity discusses the preparing, investigating, responding and transforming (PIRT) security life cycle approach along with the approach to transform organizational security to strengthen defenses and integrate cyber security with security governance, risk and compliance management. *Transforming Cybersecurity* discusses various threats such as APTs, cyberwarfare, political activism and damage to reputation.

The day-to-day business of cyber security is IT-centric, and COBIT 5 can help senior management support and budget the implementation of cyber security strategies. The financial impact of cybercrime justifies rethinking cyber security. This book describes the legal and regulatory impacts, in addition to societal impacts, of cybercrime in detail. It is also important to identify systemic weaknesses to understand how attacks and security breaches happen. The book provides a list of typical threats, vulnerabilities and risk, which is very useful for security practitioners.

Transforming Cybersecurity explains the risk-based categorization of organizational controls, social controls, technical controls and process controls, along with the COBIT 5 processes that apply to cyber security. Attack and incident data should be treated as learning materials and not just forensic evidence. Past attacks and incidents should be analyzed and integrated into the risk management process. Among the types of risk discussed in this book are organizational design and structural risk; governance, compliance and control risk; cultural risk; social risk; people risk; risk associated with human factors and all forms of technical risk.

The publication also explains developing a business case for a cyber security governance framework and the application of the five COBIT 5 Principles for better cyber security governance. *COBIT® 5 for Information Security* provides a general catalog of information security principles, which are enumerated in detail in *Transforming Cybersecurity.*

A cyber security policy should give a sense of direction and mission rather than outlining any lower-level management practices and activities. This book details the components of a cyber security policy along with the cyber security management processes across COBIT 5. Even though cyber security forms part of a corporate

Reviewed by Ravi Ayappa, Ph.D., CISA, CRISC, CISM, who is currently a principal security consultant with Cognizant Technology Solutions based in the United States. Over the last 20 years of his career, he has worked in the domains of governance, risk and compliance consulting, Internet of Things security, infrastructure security, application security, business continuity planning and disaster recovery, and information and communications technology security in Asia, Europe and the United States across various industries and the military. He is also a voluntary instructor for certification courses at the ISACA® Detroit (Michigan, USA) Chapter.

Enjoying this article?

- **Learn more about, discuss and collaborate on cyber security in the Knowledge Center.** *www.isaca.org/cybersecurity-topic*

security function, security as a whole is more of a sociotechnical function. The book addresses security management from the strategic outlook to the day-to-day practices and activities required to implement and maintain cyber security in an organizational context. This book explains the necessary people, skills and competencies for security managers and end users, along with a cyber security training program.

Assurance ensures that cyber security is designed, implemented, maintained and transformed in a manner that is consistent with all aspects of governance, risk and compliance. The book explains that cyber security should be reviewed frequently to validate the overall control set in terms of design and effectiveness. Management, risk management and internal audit are the three lines of defense in the review process. Auditors should be fully trained in the collection and preservation of evidence and understand the nuances applicable in any particular jurisdiction before attempting forensic or investigative work.

Transforming Cybersecurity shows that from an end-to-end perspective of the enterprise, cyber security will transform the organizational, technical, process, social and behavioral contexts and the relative risk position with regard to attacks, breaches and incidents. Cyber security measures applied to the COBIT 5 framework should be regularly evaluated for their systemic significance, their interdependencies with other security measures and overall risk vs. expected benefits. The book describes eight guiding principles of transforming cyber security, including the establishment of cyber security governance, end-user behavioral patterns and cultural values.

Appendix A of the book gives details of the mappings of COBIT 5 and *COBIT® 5 for Information Security* to cyber security. Appendix B covers intelligence, investigations and forensics in cyber security. The authors of this book provide detailed, step-by-step guidance to address cyber security issues and apply the relevant parts of COBIT 5 to those issues.

Editor's Note

Transforming Cybersecurity is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.